Volume: 5 Issue: X Month of publication: October 2017

DOI: http://doi.org/10.22214/ijraset.2017.10116

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X, October 2017- Available at www.ijraset.com

Analysis of Data Security and Privacy Issues in Cloud Computing Technology

Dr.P.Vijaya karthick[1], K.Suresha[2]
[1]*Proffessor,Dept.of Information Science and Engineering,Sir M V I T,Bangalure,Karnataka,India*
[1]*Lecturer, Dept.of Computer Science and Engineering,D R R G P T,Davangere,Karnataka,India*

***Abstract:** Information security and privacy are equally extremely important issues in IT industry. In the cloud processing technology, it becomes especially critical since the information is situated in various places even in the whole globe. Information security and privacy protection are the two major facets of user's considerations in regards to the cloud processing technology. However several methods on the issues in cloud processing have already been investigated in academics and industries, information safety and privacy safety are getting more crucial for future years growth of cloud processing in government, market and business. Information protection and privacy protection problems are strongly related equally hardware or equipment or electronics and computer software or application in the cloud architecture. This study is to examine various information protection methods and difficulties from both computer software or application and hardware or equipment or electronics factors for guarding information in the cloud and seeks at improving the information protection and solitude safety for the reliable cloud environment. In this research paper, we create a relative evaluation of the present research work regarding the data security and privacy issues found in the cloud computing technology.*

***Keywords:** Privacy, Malicious, Access Control, Security, Fine-Grained.*

I. INTRODUCTION

Cloud computing has been envisioned as another generation paradigm in computation. In the cloud computing environment, both applications and resources are delivered on demand over the Internet as services. Cloud is definitely an environment of the hardware and software resources in the data centers that offer diverse services over the network or the Internet to satisfy user's requirements [1].The explanation of "cloud computing" from the National Institute of Standards and Technology (NIST) [2] is that cloud computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Based on the explanation, cloud computing supplies a convenient on-demand network usage of a shared pool of configurable computing resources. Resources refer to computing applications, network resources, platforms, software services, virtual servers, and computing infrastructure. Cloud computing can be considered as a new computing archetype that will provide services on demand at a small cost. The three well-known and commonly used service models in the cloud paradigm are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In SaaS, software with the related data is deployed by a cloud service provider, and users can use it through the internet browsers. In PaaS, a service provider facilitates services to the users with some software packages that could solve the precise tasks. In IaaS,the cloud service provider facilitates services to the users with virtual machines and storage to enhance their business capabilities. Cloud computing is closely related to but not similar as grid computing [3]. Grid processing integrates diverse sources together and controls the sources with the good systems to offer high performance processing services, while cloud processing combines the processing and storage sources managed by various systems to offer services such as for example large-scaled Information storage and high performance processing to users. The overall picture of grid processing has been changed by cloud computing.

Distribution of Information is in a new method of cloud processing researching with the grid computing. Cloud processing will help companies to be taken quickly on demand. Cloud processing gets the faculties such as for example on-demand self-service, ubiquitous network accessibility, place independent reference combining, rapid reference strength, usage-based pricing, and transference of risk. These merits of cloud processing have attracted considerable pursuits from both the industrial earth and the academic research world. Cloud processing engineering is changing the way to work in the world. Cloud processing is quite promising for the IT programs; but, you will find however some issues to be resolved for personal consumers and enterprises to store Information and release programs in the cloud processing environment. One of the very most significant barriers to adoption is Information protection, that will be followed closely by issues including conformity, solitude, trust, and legal issues [4, 5]. The role of institutions and institutional progress is near to solitude and protection in cloud processing [6].

Information protection has consistently been a significant problem in IT. Information protection becomes especially critical in the cloud processing environment, since Information are scattered in various models and storage units including servers, PCs, and different mobile devices such as for example wireless indicator sites and smart phones. Information protection in the cloud processing is more difficult than Information protection in the standard data systems. To really make the cloud processing be followed by consumers and enterprise, the protection issues of consumers should really be fixed first to make cloud environment trustworthy. The reputable environment is the basic prerequisite to gain assurance of consumers to undertake this type of technology. Latif et al. discussed the evaluation of cloud processing dangers [7]. Before the info protection issues are discussed, the features of cloud processing are analyzed first. Cloud processing is also referred to as on-demand service. In the cloud processing environment, there is a cloud service provider that facilitates companies and manages the services. The cloud company facilitates all the companies over the Internet, while customers use companies for satisfying their company wants and then spend the service provider accordingly. Cloud processing environment provides two basic types of features: processing and Information storage. In the cloud processing environment, customers of cloud companies do not require anything and they are able to obtain access to their Information and end their processing projects only through the Internet connectivity. During the usage of the info and processing, the customers do not know where in actuality the Information are kept and which models execute the processing tasks. Arriving at Information storage, Information safety and protection are the principal factors for getting user's trust and creating the cloud engineering successfully used. Numerous Information rights and Information protection methods have been proposed in the research area of cloud computing. But, Information safety related methods need to be further enhanced. Solutions of cloud processing are given across the whole processing spectrum. Nowadays, companies and companies are moving and extending their company by adopting the cloud processing to reduce their cost. This will donate to free more man-powers to target on making proper differentiation and company team of labor is clearer.The cloud keeps growing consistently since it might provide high performance computational companies at cheaper rates. Popular IT companies such as for example Microsoft (http://azure.microsoft.com/), Amazon (http://aws.amazon.com/), Google (https://cloud.google .com/), and Rake space (http://www.rackspace.com/) have presented cloud support on the Internet. The concept of cloud has numerous implementations based on the services from support providers. For instance, Bing Apps Engine, Microsoft Azure, and Amazon Heap are common implementations of cloud computing given by cloud support vendors, that's, Bing, Microsoft, and Amazon companies. Besides, the ACME enterprise implemented VMware based v-Cloud for letting numerous companies to talk about computing resources. According to the difference of access scope, cloud can be divided into three types: *public cloud, private cloud,* and *hybrid cloud.*

Public cloud is because the home of supplier and can be used in public places, personal cloud refers to being the home of a company, and hybrid cloud may be the blends of community and personal cloud. Most of the existing cloud companies are offered by large cloud service businesses such as Bing, Amazon, and IBM. An exclusive cloud is really a cloud in which only the approved users may accessibility the companies from the provider. In the pubic cloud anybody can utilize the cloud companies although the hybrid cloud contains the concept of both community and personal clouds. Cloud processing may save an organization's time and income, but trusting the system is more essential since the actual asset of any firm is the information which they reveal in the cloud to utilize the required companies by placing it both right in the relational repository or ultimately in a relational repository via an application. Cloud processing delivers several features that require unique attention in regards to trusting the system. The trust of the entire process depends upon the information defense and prevention techniques utilized in it. Numerous different resources and techniques have already been tested and introduced by the scientists for information defense and prevention to achieve and take away the hurdle of trust but you will find still breaks which require attention and are expected to be arranged by making these techniques far better and effective. The meaning of safety is plentiful. Safety may be the mix of confidentiality, the prevention of the unauthorized disclosure of data, integrity, the prevention of the unauthorized amendment or deletion of data, and supply, the prevention of unauthorized withholding of data [8].The key issues in the cloud processing contain reference safety, reference management, and reference monitoring. Currently, you will find no typical rules and regulations to deploy purposes in the cloud, and there is too little standardization get a grip on in the cloud. Numerous novel techniques have been designed and applied in cloud; nevertheless, these techniques flunk of ensuring total safety due to the character of the cloud environment.

The natural issues of Information security, governance, and administration with respect to get a grip on in the cloud computing are mentioned in [9]. Sunlight et al. [10] outlined the key security, solitude, and trust issues in the existing environment of cloud computing and help customers to recognize the concrete and intangible threats related to its use. According to the writers, you can find three major potential threats in cloud computing, particularly, security, solitude, and trust. Security plays a vital role in the present period of extended considered perspective of computing as a utility. It may be split into four subcategories: *safety* mechanisms, cloud server monitoring or tracing, data confidentiality, and avoiding malicious insiders' illegal operations and service hijacking.

A data safety construction for cloud processing communities is proposed [11]. The experts primarily mentioned the safety issues linked to cloud data storage. Additionally, there are some patents about the info storage safety methods [12]. Younis and Kifayat offer a survey on protected cloud processing for important infrastructure [13]. A security and solitude construction for RFID in cloud processing was proposed for RFID engineering incorporated to the cloud processing [14],that'll mix the cloud processing with the Net of Things. In a nutshell, the foremost issues in cloud data safety include data solitude, data safety, data availability, data area, and protected transmission. The safety problems in the cloud include threats, data loss, service disruption, outside harmful attacks, and multitenancy issues [15]. Chen and Zhao [16] analyzed solitude and data safety issues in the cloud processing by concentrating on solitude safety, data segregation, and cloud security. Information safety issues are largely at SPI (SaaS, PaaS, and IaaS) stage and the important concern in cloud processing is data sharing.

In this paper, we will review various safety methods and difficulties for information storage safety and solitude security in the cloud computing environment. As Figure 1 shows, this report presents a comparative research examination of the existing research work regarding the methods used in the cloud computing through information safety aspects including information reliability, confidentiality, and availability. Information solitude problems and technologies in the cloud will also be studied, since information solitude is usually supported with information security. Relative studies on information safety and solitude could help improve the user's trust by getting information in the cloud computing environment.

II. DATA INTEGRITY

Data reliability is one of the most important aspects in any data system. Usually, data reliability indicates defending data from unauthorized erasure, change, or fabrication. Controlling entity's admittance and rights to certain enterprise sources assures that useful data and companies are not abused, misappropriated, or stolen. data reliability is simply accomplished in a standalone system with an individual database. Information reliability in the standalone system is maintained via repository restrictions and transactions, that is frequently completed by a repository management system (DBMS). Transactions must follow ACID (atomicity, consistency, solitude, and durability) qualities to make certain data integrity. Many listings help ACID transactions and may maintain data integrity. Authorization is used to regulate the accessibility of data. It is the process through which a method decides what degree of accessibility a certain authenticated user must need certainly to protected sources controlled by the system. Information reliability in the cloud system indicates keeping data integrity. The info shouldn't be lost or revised by unauthorized users. Information reliability is the foundation to provide cloud computing service such as for example SaaS, PaaS, and IaaS. Besides data storage of large-scaled data, cloud computing atmosphere frequently gives data running service. Information reliability may be received by techniques such as for example RAID-like methods and digital signature. Owing to the large level of entities and accessibility items in a cloud atmosphere, authorization is a must in assuring that only licensed entities may talk with data. By steering clear of the unauthorized accessibility, agencies can achieve greater confidence in data integrity. The tracking systems provide the greater exposure into deciding who or what could have altered data or system data, possibly affecting their integrity. Cloud computing companies are trusted to maintain data reliability and accuracy. Nevertheless, it is necessary to create the third party supervision process besides users and cloud service providers. Verifying the reliability of data in the cloud remotely is the perquisite to utilize applications. Bowers et al. planned a theoretical construction "Proofs of Retrievability" to understand the rural data reliability checking by combining error modification rule and spot-checking [17]. The HAIL system employs POR process to test the storage of data in various clouds, and it can ensure the redundancy of various copies and know the availability and reliability checking [18]. Schiffman et al. planned trusted program component (TPM) rural checking to test the data reliability remotely [19].

III.DATA CONFIDENTIALITY

Information confidentiality is essential for people to store their private or confidential data in the cloud. Authentication and entry control methods are accustomed to ensure data confidentiality. The data confidentiality, certification, and entry control dilemmas in cloud processing might be resolved by raising the cloud reliability and trustworthiness [20]. Since the people do not trust the cloud vendors and cloud storage company vendors are practically impossible to get rid of potential insider danger, it's very harmful for people to store their painful and sensitive data in cloud storage directly. Easy security is confronted with the key administration issue and cannot support complex demands such as for example query,parallel adjustment, and fine-grained authorization.

A. Homomorphic Encryption.]

Encryption is usually applied to guarantee the confidentiality of data. Homomorphic encryption is some sort of security program proposed by Rivest et al [21].

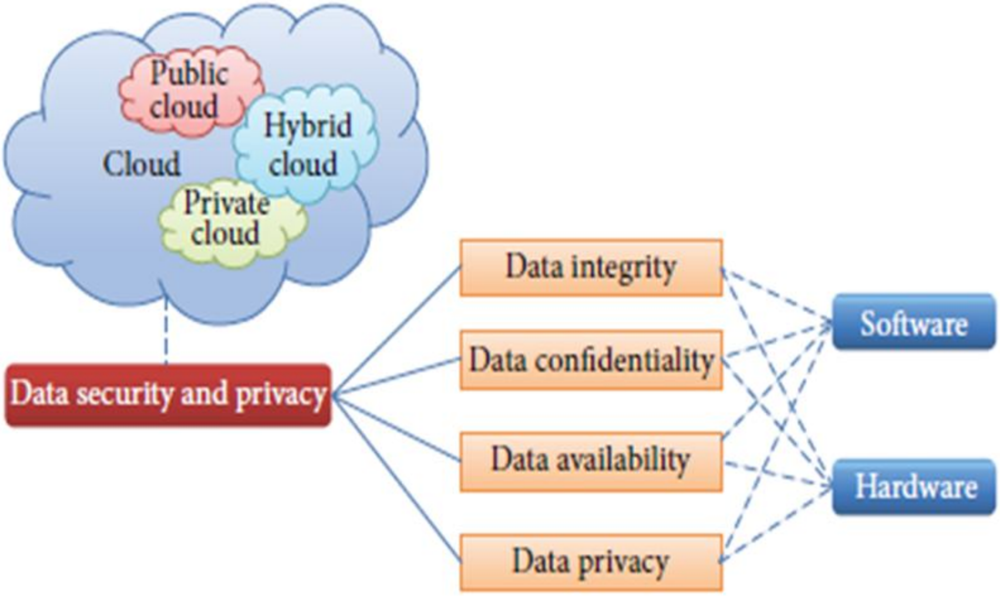

Figure-1:Organization of data security and privacy in cloud computing

It guarantees that the cipher text algebraic operation answers are in keeping with the apparent operation after security results; besides, the entire method does not want to decrypt the data. The implementation with this strategy could effectively solve the confidentiality of information and information operations in the cloud. Gentry firstly proposed the fully homomorphic security strategy [22], which can do any operation that may be performed in apparent text without decrypting. It is an essential discovery in the homomorphic security technology. But, the security program requires really complex calculation, and the price of research and storage is quite high. This results in the fact that the fully homomorphic security continues to be definately not real applications. A cryptographic algorithm named Diffie-Hellman is proposed for protected interaction [23], which can be quite dissimilar to the key circulation administration mechanism. For more freedom and enhanced security, a cross strategy that mixes numerous security methods such as RSA, 3DES, and arbitrary number turbine has been proposed [24]. RSA is helpful for establishing protected interaction relationship through electronic signature centered validation while 3DES is particularly helpful for security of stop data. Besides, a few security methods for ensuring the security of individual information in the cloud research are discussed [25].

B. Encrypted Search and Database

Because the homomorphic encryption algorithm is inefficient, researchers change to study the applications of confined homomorphic encryption algorithm in the cloud environment. Protected search is just a frequent operation. Manivannan and Sujarani [26] have planned a lightweight device for database encryption called transposition, alternative, folding, and shifting (TSFS) algorithm. However, because the numbers of keys are improved, the quantity of computations and running also increases. In-Memory Database encryption technique is planned for the privacy and security of painful and sensitive Information in untrusted cloud atmosphere [27]. A synchronizer exists between the owner and the customer for seeking access to the data. Client would demand a key from the synchronizer to decrypt the secured discussed Information it gets from the owner. The synchronizer is utilized to store the correlated discussed Information and the keys separately. A shortcoming of this technique is that the setbacks arise due to the extra conversation with the central synchronizer. However, this restriction can be mitigated by adopting party encryption and through reducing conversation between nodes and synchronizer. Huang and Tso [28] planned an asymmetric encryption device for databases in the cloud. In the planned device, the commutative encryption is used on Information more often than once and the order of public/private key used for encryption/decryption doesn't matter. Reencryption device can also be utilized in the planned scheme which implies that the cipher-text Information is secured yet again for duality. Such schemes are very helpful in the cloud applications wherever privacy is just a key concern. A privacy-preserving multikeyword ranked search approach around secured cloud Information was planned [29], which can search the secured cloud Information and position the search results without loss of the user's privacy.

C. Distributive Storage

Distributive storage of data is also a encouraging approach in the cloud environment. AlZain et al. [30] mentioned the protection problems related to data privacy in the cloud computing including strength of data, intrusion, and option of service in the cloud. To guarantee the data strength, one option could possibly be to keep data in numerous clouds or cloud databases. The info to be secured from internal or additional unauthorized entry are divided into portions and Shamir's secret algorithm is used to produce a polynomial purpose against each chunk. Ram and Sreenivaasan [31] have planned a technique called protection as a service for securing cloud data. The planned technique can achieve maximum protection by splitting the user's data into pieces. Thesedata portions are then encryptedand stored in divided databases which follow the thought of data distribution over cloud. Because each section of data is secured and individually distributed in databases over cloud, this gives enhanced protection against various kinds of attacks. Arfeen et al. [32] explain the distribution of sources for cloud computing on the basis of the designed productive measurement. The designed rating technique is on the basis of the system design and the precise channels for the inward and outgoing traffic and slowly changing the sources based on the user needs. Tailored rating depends upon the computing sources and storage resources. Because of the variable nature of systems, the allocation of sources at a certain time on the basis of the designed productive strategy doesn't remain optimal. The sources might raise or decrease, so the device has to optimize improvements in the consumer requirement often traditional or on-line and the source connectivity.

D. Hybrid Technique

A hybrid approach is planned for data confidentiality and strength [33], which uses both essential discussing and certification techniques. The connectivity between the consumer and the cloud supplier may be built more secure by applying effective essential discussing and certification processes. RSA public essential algorithm can be utilized for secure distribution of the secrets between the consumer and cloud service providers.A three-layered data protection approach is planned [34]: the first coating is employed for authenticity of the cloud individual possibly by one factor or by two factor authentications; the 2nd coating encrypts the user's data for ensuring safety and solitude; and the third coating does fast healing of data through a fast decryption process. An event-based isolation of important data in the cloud strategy is planned [35], TrustDraw, a clear protection extension for the cloud which combines electronic machine introspection (VMI) and trusted computing (TC).

E. Data Concealment

Information concealment could also be used to keep the information confidentiality in the cloud. Delettre et al.[36] presented a concealment principle for sources security.Data concealment approachesmerge actual information with the aesthetic phony information to falsify the actual data's volume.However, authorized people can certainly distinguish and split the phony information from the actual data. Information concealment practices improve the overall level of actual information but provide increased protection for the private data. The objective of information concealment is to really make the actual information safe and protected from harmful people and attackers. Watermarking method may function as a key for the actual data. Only the authorized people have important of watermarking, so the certification of people is the key to guarantee the correct information to be available for correct users.

F. Deletion Confirmation

Erasure verification implies that data could not be recovered when people erase their data following the deletion confirmation. The thing is really critical, because multiple duplicate exists in the cloud for the protection and ease of data recovery. When people erase their data with verification, all the copies of data must certanly be wiped at the exact same time. Nevertheless, there are some data recovery technologies that could recover the info wiped by people from the hard disks. Therefore the cloud storage providers must ensure that the wiped data of people could not be recovered and utilized by different unauthenticated users. To prevent the data be recovered and unauthenticatedly applied, a possible strategy is always to encrypt the info before publishing to the cloud storage space. FADE process [37] is based on technologies such as for example Ephemerizer. In the machine, data are protected before they're downloaded to the cloud storage. When people choose to erase their data, the machine only to apply the specific technique to all the space for storage could be coveredwith newdata for changing the deletion operation.

IV.DATA AVAILABILITY

Information availability suggests the next: when accidents such as for example hard disk drive injury, IDC fire, and system problems occur, the extent that user's data can be utilized or recovered and how a consumers examine their data by practices as opposed to with regards to the credit assure by the cloud company alone. The issue of storing data within the transboarder hosts is a critical concern of clients since the cloud sellers are governed by the neighborhood laws and, therefore, the cloud clients ought to be conscious of those laws. Furthermore, the cloud company should guarantee the info safety, especially data confidentiality and integrity. The cloud company should share all such concerns with the customer and build trust relationship in that connection. The cloud vendor should give guarantees of data safety and describe jurisdiction of local laws to the clients. The key emphasis of the paper is on these data dilemmas and challenges which are associated with data storage location and their separation, price, availability, and security. Locating data might help consumers to increase their trust on the cloud. Cloud storage offers the transparent storage company for consumers, that may decrease the difficulty of cloud, but it also diminishes the get a grip on power on data storage of users. Benson et al. studied the proofs of geographical reproduction and succeeded in finding the info stored in Amazon cloud [38].

A. Reliable Storage Agreement

The most common abnormal conduct of untrusted storage is that the cloud service suppliers may toss area of the user's upgrade Information, that will be hard to be checked by just depending on the simple Information encryption. Also, a good storage deal needs to guide concurrent adjustment by numerous users. Mahajan et al. planned Resource which can promise Fork-Join-Causal-Consistency and ultimate reliability [39]. It can effortlessly fight attacks such as for instance discarding and it may support the implementation of other protection protections in the trusted cloud storage environment (such as Amazon S3). Feldman et al. planned SPORC [40], which can implement the safe and reliable real-time connection and cooperation for numerous customers with the aid of the trusted cloud environment, and untrusted cloud servers can only accessibility the protected data. But, function types supported by reliable storage process support are restricted, and a lot of the calculations can only arise in the client.

B. Reliability of Hard-Drive

Hard-drive is currently the key storage media in the cloud environment. Consistency of hard drives formulates the foundation of cloud storage. Pinheiro et al. studied the problem charge of hard-drives on the basis of the historic information of hard-drive [41]. They unearthed that the problem charge of hard-drives is not strongly relevant to the heat and the frequency to be properly used, as the problem charge of hard-drives has got the powerful clustering characteristics. Recent SMART device couldn't predict the problem charge of hard disks. Tsai et al. studied the correlation between the smooth problem and hard problem of hard drives, and they also unearthed that the smooth problem couldn't predict the hard problems of hard disk drives specifically [42], only about 1/3 likelihood that hard problems follow the smooth errors.

V. DATA PRIVACY

Privacy is the ability of someone or group to secure them or information about themselves and thus show them selectively [43]. Privacy has the following elements.(i) When: a topic might become more concerned with the current or future data being exposed than data from the past. (ii) How: a user may be comfortable if his/her friends may personally request his/her data, but the user might in contrast to alerts to be delivered quickly and frequently.(iii) Degree: a user might rather have his/her data reported as an uncertain place rather than accurate point. In commerce, consumer's situation and solitude need to be protected and applied appropriately. In agencies, solitude entails the application of laws, elements, criteria, and operations by which individually identifiable data is handled [44].

In the cloud, the solitude means when users visit the sensitive and painful data, the cloud services may reduce potential adversary from inferring the user's conduct by the user's visit product (not direct data leakage). Scientists have dedicated to Oblivious RAM (ORAM) technology. ORAM technology visits several copies of data to full cover up the true visiting aims of users. ORAM has been commonly utilized in software safety and has been utilized in guarding the solitude in the cloud as a promising technology.

Stefanov et al. planned that the course ORAM algorithm is state-of-the-art implementation [45]. The solitude issues vary in accordance with different cloud scenarios and can be split into four subcategories [44, 46, 47] the following:
(i) how to enable users to have control around their data once the data are located and processed in cloud and prevent robbery, nefarious use, and unauthorized resale,(ii) how exactly to promise data replications in a jurisdiction and consistent state, where replicating person data to numerous acceptable locations can be an normal selection, and prevent data reduction, loss, and unauthorized modification or manufacturing, (iii) which party is accountable for ensuring appropriate needs for personal data, (iv) to what degree cloud subcontractors are involved with running which can be effectively identified, checked, and ascertained.

A. Service Abuse

Support punishment implies that attackers may punishment the cloud support and purchase added data or ruin the interests of different users. Individual data may be abused by different users. Deduplication technology has been generally used in the cloud storage, meaning that exactly the same data often were kept when but shared by numerous different users. This will reduce steadily the space for storing and decrease the cost of cloud support services, but attackers may accessibility the information by understanding the hash signal of the kept files. Then, it is possible to leak the painful and sensitive data in the cloud. Therefore evidence of ownership strategy has been proposed to test the authorization of cloud consumers [48]. Enemies can result in the price improve of cloud service. Fraudulent reference use is some sort of strike on the cost for cloud service. Enemies may digest the particular data to increase the price for cloud support payment. Idziorek et al. proposed this question and researched on the detection and identification of scam reference use [49].

B. Averting Attacks.

The cloud computing facilitates enormous amount of provided sources on the Internet. Cloud programs should be capable of averting Refusal of Company (DoS) attacks. Shen et al. examined necessity of protection solutions in cloud computing [50]. The writers suggest integrating cloud solutions for trusted computing program (TCP) and trusted program help solutions (TSS). The trusted design should carry traits of confidentiality, dynamically making trust domains and vibrant of the services. Cloud infrastructures involve that individual moves their data into cloudmerely based on trust. Neisse et al. examined indifferent episodes circumstances on Xen cloud program to gauge cloud solutions based on trust. Security of data and rely upon cloud computing is the main element point for its broader adoption [51]. Yeluri et al. dedicated to the cloud solutions from protection viewpoint and investigated protection challenges in cloud when deploying the solutions [52]. Personality administration, data healing and administration, protection in cloud confidentiality,trust, exposure, and application architecture are the main element factors for ensuring protection in cloud computing.

C. Identity Management

Cloud computing supplies a podium to make use of wide variety of Internet-based companies [53]. But besides their advantages, additionally, it advances the safety threat each time a respected 3rd party is involved. By involving a dependable 3rd party, there's a chance of heterogeneity of consumers which affects safety in the cloud. A probable treatment for this problem might be to employ a respected 3rd party independent method for Identification Administration to make use of identity Information on untrusted hosts. Squicciarini et al. focused on issues of Information loss and lack of privacy in cloud computing [54]. Various degrees of rights can be used to avoid Information loss and privacy loss in the cloud. Cloud computing gives new organization companies that are based on demand. Cloud communities have already been built through active virtualization of equipment, computer software, and datasets. Cloud safety infrastructure and the confidence name administration enjoy an important position to update the cloud companies [55]. The Access to the internet safety, machine entry safety, plan entry safety, and database safety are the key safety problems in the cloud.

VI.CONCLUSION

Cloud processing is a promising and emerging engineering for the next generation of IT applications. The barrier and hurdles toward the rapid development of cloud research are data protection and solitude issues. Reducing data storage and handling cost is an obligatory requirement of any firm, while examination of data and data is always the main responsibilities in all of the businesses for decision making. So no businesses will move their data or data to the cloud before the confidence is made involving the cloud company vendors and consumers. A number of practices have already been planned by experts for data security and to attain best degree of data protection in the cloud. However, you can find still several spaces to be filled by creating these practices more effective. More perform is required in your community of cloud research to create it adequate by the cloud company consumers. This paper interviewed various practices about data protection and solitude, emphasizing the data storage and used in the cloud, for data security in the cloud research surroundings to build confidence between cloud company vendors and consumers.

REFERENCES

[1] N. Leavitt, “Is cloud computing really ready for prime time?”Computer, vol. 42, no. 1, pp. 15–25, 2009.

[2] P.Mell and T. Grance, “The nist definition of cloud computing,”National Institute of Standards and Technology, vol. 53, no. 6,article 50, 2009.

[3] F. Berman,G.Fox, andA. J. G. Hey, Grid Computing:Making theGlobal Infrastructure a Reality, Volume 2, JohnWiley and sons,2003.

[4] M. A. Shah, R. Swaminathan, and M. Baker, “Privacy-preserving audit and extraction of digital contents,” IACR Cryptology EPrint Archive, vol. 186, 2008.

[5] Z. Xiao andY.Xiao, “Security and privacy in cloud computing,” IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp.843–859, 2013.

[6] N. Kshetri, “Privacy and security issues in cloud computing: the role of institutions and institutional evolution,” Telecommunications Policy, vol. 37, no. 4-5, pp. 372–386, 2013.

[7] R. Latif, H. Abbas, S. Assar, and Q. Ali, “Cloud computing risk assessment: a systematic literature review,” in Future Information Technology, pp. 285–295, Springer, Berlin, Germany, 2014.

[8] A. Aviˇzienis, J. Laprie, B. Randell, and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing,”IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11–33, 2004.

[9] Z. Mahmood, “Data location and security issues in cloud computing,” in Proceedings of the 2nd International Conference on Emerging Intelligent Data andWeb Technologies (EIDWT ’11),pp. 49–54, IEEE, September 2011.

[10] D. Sun, G. Chang, L. Sun, and X. Wang, “Surveying and analyzing security, privacy and trust issues in cloud computing environments,” in Proceedings of the International Conference on Advanced in Control Engineering and Information Science (CEIS ’11), pp. 2852–2856, chn, August 2011.

[11] A. Pandey, R. M. Tugnayat, and A. K. Tiwari, “Data Security Framework for Cloud Computing Networks,” International Journal of Computer Engineering & Technology, vol. 4, no. 1, pp. 178–181, 2013. [12] D. A. Klein, “Data security for digital data storage,” U.S. Patent Application 14/022,095, 2013.

[12] M. Y. A. Younis and K. Kifayat, “Secure cloud computing for critical infrastructure: a survey,” Tech. Rep., Liverpool John Moores University, Liverpool, UK, 2013.

[13] S. Kardas¸, S. C¸elik, M. A. Bing¨ol, and A. Levi, “A new security and privacy framework for RFID in cloud computing,” in Proceedings of the 5th IEEE International Conference on Cloud Computing Technology and Science (CloudCom '13), Bristol , UK,2013.

[14] A. Behl, “Emerging security challenges in cloud computing: an insight to cloud security challenges and their mitigation,” in Proceedings of the World Congress on Information and Communication Technologies (WICT ’11), pp. 217–222, IEEE,December 2011.

[15] D. Chen and H. Zhao, “Data security and privacy protection issues in cloud computing,” in Proceeding of the International Conference on Computer Science and Electronics Engineering (ICCSEE '12), vol. 1, pp. 647–651,Hangzhou, China,March 2012.

[16] K. D. Bowers, A. Juels, and A. Oprea, “Proofs of retrievability: theory and implementation,” in Proceedings of the ACM Workshop on Cloud Computing Security (CCSW’09), pp. 43–53, November 2009.

[17] K. D. Bowers, A. Juels, and A. Oprea, “HAIL: a high-availability and integrity layer for cloud storage,” in Proceedings of the 6th ACMconference onComputer andCommunications Security, pp. 187–198, ACM, Chicago, Ill, USA, November 2009.

[18] J. Schiffman, T. Moyer, H. Vijayakumar, T. Jaeger, and P. McDaniel, “Seeding clouds with trust anchors,” in Proceedings of the ACM workshop on Cloud computing security workshop (CCSW ’10), pp. 43–46, ACM, October 2010.

[19] D. H. Rakesh, R. R. Bhavsar, and A. S. Thorve, “Data security over cloud,” International Journal of Computer Applications, no.5, pp. 11–14, 2012.

[20] R. L. Rivest, L. Adleman, andM. L.Dertouzos, “On data banks and privacy homomorphisms,” Foundations of Secure Computation,vol. 4, no. 11, pp. 169–180, 1978.

[21] C. Gentry, A fully homomorphic encryption scheme [Ph.D.thesis], Stanford University, 2009.

[22] D. Boneh, “The decision Diffie-Hellman problem,” in Algorithmic NumberTheory, vol. 1423, pp. 48–63, Springer, 1998.

[23] A. Kaur and M. Bhardwaj, “Hybrid encryption for cloud database security,” Journal of Engineering Science Technology,vol. 2, pp. 737–741, 2012.

[24] R. Arora, A. Parashar, and C. C. I. Transforming, “Secure user data in cloud computing using encryption algorithms,” Internationa Journal of Engineering Research and Applications, vol. 3, no. 4, pp. 1922–1926, 2013.

[25] D. Manivannan and R. Sujarani, “Light weight and secure database encryption using tsfs algorithm,” in Proceedings of

[26] the International Conference on Computing Communication and Networking Technologies (ICCCNT '10), pp. 1–7, IEEE, 2010.

[27] F. Pagano and D. Pagano, “Using in-memory encrypted databases on the cloud,” in Proceedings of the 1st IEEE International Workshop on Securing Services on the Cloud (IWSSC ’11), pp. 30–37, September 2011.

[28] K.Huang and R. Tso, “A commutative encryption scheme based on ElGamal encryption,” in Proceedings of the 3rd International Conference on Information Security and Intelligent Control (ISIC ’12), pp. 156–159, IEEE, August 2012.

[29] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data,” IEEE Transactions on Parallel andDistributed Systems, vol. 25, no. 1, pp. 222–233, 2014.

[30] M. A. AlZain, B. Soh, and E. Pardede, “Mcdb: using multiclouds to ensure security in cloud computing,” in Proceedings of the IEEE 9th International Conference on Dependable, Autonomic and Secure Computing (DASC ’11), pp. 784–791, 2011.

[31] C. P. Ram and G. Sreenivaasan, “Security as a service (sass):securing user data by coprocessor and distributing the data,”in Proceedings of the 2nd International Conference on Trendz in Information Sciences and Computing, (TISC '10), pp. 152–155, IEEE, December 2010.

[32] M. Asad Arfeen, K. Pawlikowski, and A. Willig, “A framework for resource allocation strategies in cloud computing environment,” in Proceedings of the 35th Annual IEEE International Computer Software and Applications Conference Workshops (COMPSACW’11), pp. 261–266, July 2011.

[33] A. Rao, “Centralized database security in cloud,” International Journal of Advanced Research in Computer and Communication Engineering, vol. 1, pp. 544–549, 2012.

[34] E. M.Mohamed, H. S. Abdelkader, and S. El-Etriby, “Enhanced data security model for cloud computing,” in Proceedings of the 8th International Conference on Informatics and Systems (INFOS '12), pp. CC-12–CC-17, IEEE, 2012.

[35] S. Biedermann and S. Katzenbeisser, “POSTER: event-based isolation of critical data in the cloud,” in Proceedings of the ACM SIGSAC Conference on Computer & Communications Security,pp. 1383–1386, ACM, 2013.

[36] C. Delettre, K. Boudaoud, and M. Riveill, “Cloud computing, security and data concealment,” in Proceedings of the 16th IEEE Symposium on Computers and Communications (ISCC ’11), pp. 424–431, Kerkyra, Greece, July 2011.

[37] Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, “Fade: secure overlay cloud storage with file assured deletion,” in Security and Privacy in Communication Networks, pp. 380–397, Springer, New York, NY, USA, 2010.

[38] K. Benson, R. Dowsley, and H. Shacham, “Do you know where your cloud files are?” in Proceedings of the 3rd ACMworkshop on Cloud computing security workshop, pp. 73–82, ACM, October 2011.

[39] P. Mahajan, S. Setty, S. Lee et al., “Depot: cloud storage with minimal trust,”ACMTransactions on Computer Systems, vol. 29, no. 4, article 12, 2011.

[40] A. J. Feldman,W. P. Zeller, M. J. Freedman, and E. W. Felten, “SPORC: group collaboration using untrusted cloud resources,”in Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation (OSDI ’10), vol. 10, pp. 337–350, 2010.

[41] E. Pinheiro, W.-D.Weber, and L. A. Barroso, “Failure trends in a large disk drive population,” in Proceedings of the 5th USENIX conference on File and Storage Technologies (FAST '07), vol. 7, pp. 17–23.

[42] T. Tsai, N. Theera-Ampornpunt, and S. Bagchi, “A study of soft error consequences in hard disk drives,” in Proceeding of the 42ndAnnual IEEE/IFIP InternationalConference onDependable Systems and Networks (DSN '12), pp. 1–8, Boston, Mass,USA, June 2012.

[43] J. Krumm, “A survey of computational location privacy,” Personal and Ubiquitous Computing, vol. 13, no. 6, pp. 391–399,2009.

[44] S. Pearson and A. Benameur, “Privacy, security and trust issues arising from cloud computing,” in Proceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science (CloudCom ’10), pp. 693–702, IEEE, December 2010.

[45] E. Stefanov, M. van Dijk, E. Shi et al., “Path oram: an extremely simple oblivious ram protocol,” in Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, pp. 299–310, ACM, 2013.

[46] S. Paquette, P. T. Jaeger, and S. C. Wilson, “Identifying the security risks associated with governmental use of cloud computing,”Government Information Quarterly, vol. 27, no. 3, pp. 245–253, 2010.

[47] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud,” Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, 2011.

[48] C. Cachin and M. Schunter, “A cloud you can trust,” IEEE Spectrum, vol. 48, no. 12, pp. 28–51, 2011.

[49] J. Idziorek, M. Tannian, and D. Jacobson, “Attribution of Fraudulent Resource Consumption in the cloud,” in Proceedings of the IEEE 5th International Conference on Cloud Computing (CLOUD ’12), pp. 99–106, June 2012.

[50] Z. Shen, L. Li, F. Yan, and X. Wu, “Cloud computing system based on trusted computing platform,” in Proceedings of the International Conference on Intelligent Computation Technology and Automation (ICICTA ’10), vol. 1, pp. 942–945, IEEE, May 2010.

[51] R. Neisse, D. Holling, and A. Pretschner, “Implementing trust in cloud infrastructures,” in Proceedings of the 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid ’11), pp. 524–533, IEEE Computer Society, May 2011.

[52] R. Yeluri, E. Castro-Leon, R. R. Harmon, and J. Greene,“Building trust and compliance in the cloud for services,” in Proceedings of the Annual SRII Global Conference (SRII ’12), pp. 379–390, San Jose, Calif, USA, July 2012.

[53] R. Ranchal, B. Bhargava, L. B. Othmane et al., “Protection of identity information in cloud computing without trusted third party,” in Proceedings of the 29th IEEE Symposium on Reliable Distributed Systems (SRDS ’10), pp. 368–372,November 2010.

[54] A. Squicciarini, S. Sundareswaran, and D. Lin, “Preventing information leakage fromindexing in the cloud,” in Proceedings of the 3rd IEEE International Conference on Cloud Computing (CLOUD ’10), pp. 188–195, July 2010.

[55] K. Hwang and D. Li, “Trusted cloud computing with secure resources and data coloring,” IEEE Internet Computing, vol. 14,no. 5, pp. 14–22, 2010.

[56] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu” Review Article Data Security and Privacy in Cloud Computing” Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2014, Article ID 190903, 9 pages